Math100B - HW #6

Jay Ser

2026.02.19

Here's something useful:

Claim 1. *Let D be a unique factorization domain and F its field of fractions. Suppose $f(x) \in D[x]$ is primitive. Then f is irreducible in $D[x] \iff f$ is irreducible in $F[x]$.*

Proof of Claim 1. If f factors in $F[x]$, then it factors in $D[x]$ by Gauss's Lemma. Conversely, suppose f factors in $D[x]$. Since f is primitive, its factor is not a constant in D, so $f(x) = g(x)h(x)$ for nonconstant $g, h \in D[x]$. Thus f factors in $F[x]$ as well. □

1.

(a)

$x^2 + 27x + 213 \equiv x^2 + x + 1 \pmod 2$, the latter being irreducible in $\mathbb{Z}/2\mathbb{Z}$ since it is degree 2 and clearly has no roots. So $x^2 + 27x + 213$ is irreducible in $\mathbb{Q}[x]$.

(b)

$x^3 + 2x + 1$ is a degree 3 polynomial, so if it factors in $\mathbb{Q}[x]$, then it has a root in $\mathbb{Q}$. By the rational root theorem, if $r/s \in \mathbb{Q}$ with $\gcd(r, s) = 1$ is a root, then $r \mid 1$ and $s \mid 1$, i.e., $r = \pm 1$ and $s = \pm 1$, i.e.,

$$\text{The only possible roots of } x^3 + 2x + 1 \text{ are } \pm 1$$

But clearly, neither are. Hence $x^3 + 2x + 1$ is irreducible in $\mathbb{Q}[x]$.

(c)

$x^5 - 3x^4 + 3$ is irreducible by the Eisenstein criterion with $p = 3$.

2.

x^5+5x+5 is irreducible in $\mathbb{Q}[x]$ by the Eisenstein criterion with $p = 5$. Next, reducing modulo 2, $x^5+5x+5 \equiv x^5 + x + 1 \pmod 2$. $x^5 + x + 1$ clearly has no roots in $\mathbb{Z}/2\mathbb{Z}$, so if it factors, then

$$x^5 + x + 1 = (x^3 + ax^2 + bx + c)(x^2 + \alpha x + \gamma)$$

with $x^3 + ax^2 + bc + c$ and $x^2 + \alpha x + \gamma$ both irreducible.

- By Sieve of Eratosthenes or pure brute force, one can check that the only irreducible degree 2 polynomial in $\mathbb{Z}/2\mathbb{Z}$ is $x^2 + x + 1$ (all others have roots).
- Similarly, one can check that the only irreducible degree 3 polynomials in $\mathbb{Z}/2\mathbb{Z}$ are $x^3 + x^2 + 1$ and $x^3 + x + 1$.

From the two possible options for the degree 3 polynomial, one can check that

$$x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$$

in $\mathbb{Z}/2\mathbb{Z}$.

3.

In all these cases, because $f(x) := x^3 + x + 1$ is a degree 3 polynomial, it suffices to check that $x^3 + x + 1$ has roots (or lack thereof). In the following, I drop the bar notation for convenience.

(a) $\mathbf{p = 2}$

As noted in Q2, $f(x)$ has no roots in $\mathbb{Z}/2\mathbb{Z}$: $f(0) = f(1) = 1$. f is irreducible in $\mathbb{Z}/2\mathbb{Z}$.

(b) $\mathbf{p = 3}$

$f(0) = f(2) = 1$ and $f(1) = 0$, so $x - 1 = x + 2$ is the only degree one factor of f. Use the division algorithm to check that

$$x^3 + x + 1 = (x + 2)(x^2 + x + 2)$$

(c) $\mathbf{p = 5}$

$f(0) = f(2) = f(3) = 1$, $f(1) = 3$, and $f(4) = 4$, so f is irreducible in $\mathbb{Z}/5\mathbb{Z}$.

4.

It is an immediate result of the Eisenstein criterion that $x^n - p$ is irreducible for every every $n \geq 0$ and every prime integer p.

5.

There are $5^2 = 25$ monic polynomials of degree 2 in $\mathbb{Z}/5\mathbb{Z}[x]$. The ones that factor have the form $(x-a)(x-b)$ for $a, b \in \mathbb{Z}/5\mathbb{Z}$. To avoid double-counting the same polynomials, assume $a \geq b$. Then there are a total of 5, 4, 3, 2, 1 choices for a when $b = 0, 1, 2, 3, 4$, respectively. This sums to 15, so there are a total of 15 reducible degree 2 polynomials, and hence 10 irreducible degree 2 polynomials in $\mathbb{Z}/5\mathbb{Z}[x]$.